

Konfiguracja podwójnego uwierzytelniania (MFA) dla urządzeń mobilnych z systemem Android

Uniwersytet Jagielloński

Centrum Informatyki

Dział Infrastruktury Systemów Informatycznych

Data dokumentu: luty 2024, Wersja:1.1

Autorzy:

Monika Adamiec (m.adamiec@uj.edu.pl)

Estera Ambroź (estera.ambroz@uj.edu.pl)

INFORMACJA TELEADRESOWA

Centrum Informatyki, Dział Infrastruktury Systemów Informatycznych, ul. Reymonta 4, Kraków

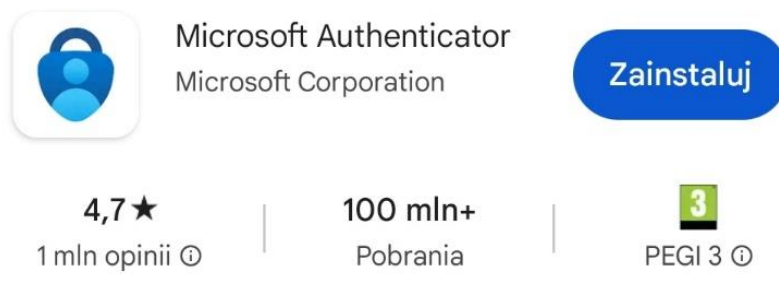
E-mail: ci@uj.edu.pl | **Web:** <https://it.uj.edu.pl>

Spis treści

Konfiguracja podwójnego uwierzytelniania (MFA) dla urządzeń mobilnych z systemem Android	1
Etap 1 - Pobieranie aplikacji na urządzenie mobilne	3
Etap 2 - Włączanie zabezpieczenia na koncie UJ	5
Etap 3 - Zgłoszenie gotowości do włączenia podwójnego uwierzytelnienia	14
Etap 4 - logowanie po włączeniu podwójnego uwierzytelniania	15
Dodatkowe czynności wymagane dla niektórych urządzeń oraz aplikacji	18
Klient synchronizacji OneDrive	18

ETAP 1 - POBIERANIE APLIKACJI NA URZĄDZENIE MOBILNE

Pierwszym krokiem, aby poprawnie rozpocząć konfigurację dwufaktorowego logowania (podwójnego uwierzytelniania), jest pobranie na swoje urządzenie mobilne (smartfon lub tablet) aplikacji **Microsoft Authenticator** ze Sklepu Play.



Po pobraniu aplikacji i jej uruchomieniu wyświetli się informacja o prywatności danych, którą należy zatwierdzić wybierając opcję *Akceptuj*. Na kolejnym ekranie należy wybrać opcję *Kontynuuj*. Nie ma konieczności wyrażania zgody na zbieranie przez aplikację dodatkowych danych.



Firma Microsoft szanuje Twoją prywatność

Zbieramy wymagane dane diagnostyczne, aby zapewnić bezpieczeństwo i aktualizację aplikacji. Nie obejmuje to żadnych danych osobowych.

Akceptuj

Oświadczenie o ochronie prywatności
firmy Microsoft



Pomóż nam ulepszyć aplikację Microsoft Authenticator

Zezwalając nam na zbieranie dodatkowych danych innych niż osobiste, możesz pomóc nam ulepszyć aplikację. Możesz włączyć lub wyłączyć tę funkcję w dowolnym momencie na stronie Ustawienia



Ulepsz aplikację,
udostępniając dane użycia
aplikacji

Kontynuuj

Oświadczenie o ochronie prywatności
firmy Microsoft

Następnie wyświetli się kolejny ekran, w którym możliwy jest wybór sposobu połączenia aplikacji z kontem uniwersyteckim.

Na tym chwilowo kończymy używanie naszej aplikacji, aż do momentu włączenia zabezpieczenia na swoim koncie na komputerze. Oznacza to, że chwilowo nie wybieramy żadnej z poniższych opcji.



Zabezpiecz swoje życie cyfrowe



Zaloguj się przy użyciu
konta Microsoft

W przypadku zalogowania się przy użyciu konta Microsoft, wszystkie zapisane hasła, adresy i inne informacje wypełniane automatycznie będą dostępne na tym urządzeniu.



Dodaj konto służbowe

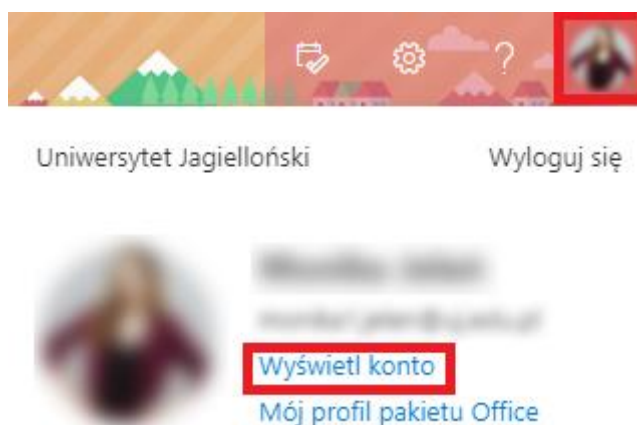


Zeskanuj kod QR

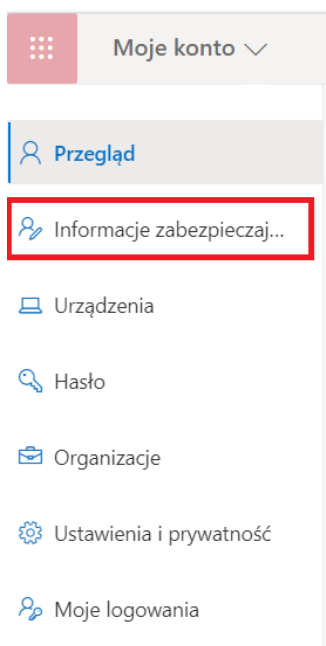
Przywróć z kopii zapasowej

ETAP 2 - WŁĄCZANIE ZABEZPIECZENIA NA KONCIE UJ

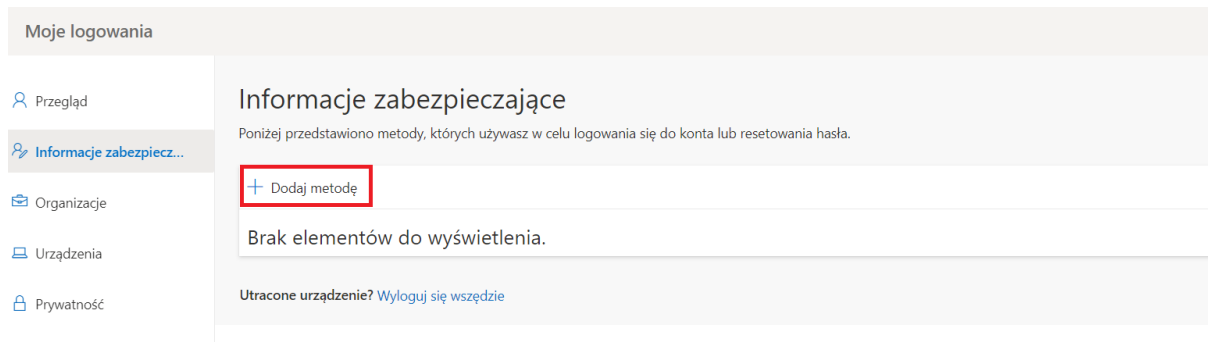
Korzystając z komputera należy otworzyć przeglądarkę internetową i zalogować się na stronie *office.com* używając uniwersyteckiego identyfikatora logowania. Następnie należy kliknąć w ikonę profilu (ze swoimi inicjałami, bądź zdjęciem), która znajduje się w prawym górnym rogu i wybrać *Wyświetl konto*.



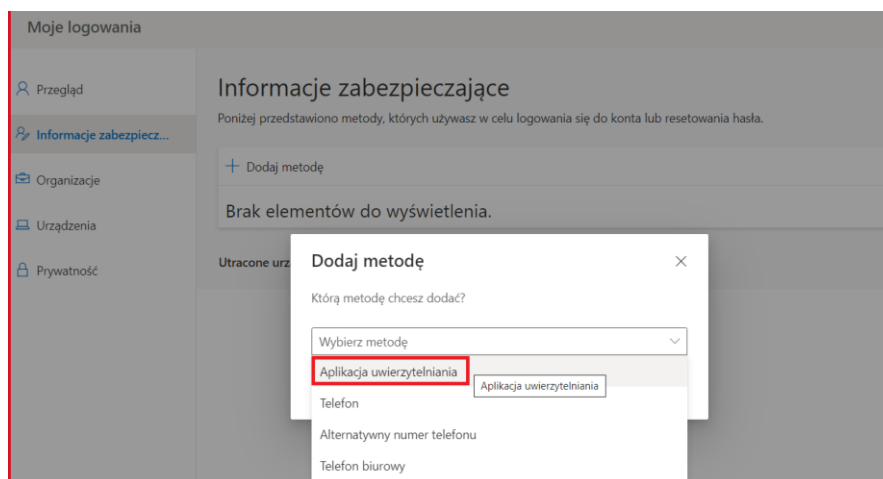
Następnie w menu po lewej stronie wybieramy *Informacje zabezpieczające*.



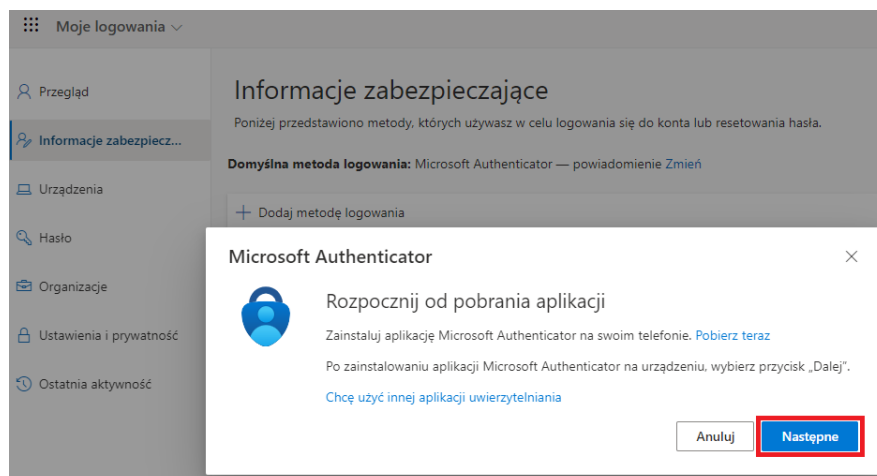
Na stronie *Informacji zabezpieczających* należy wybrać opcję *Dodaj metodę*.



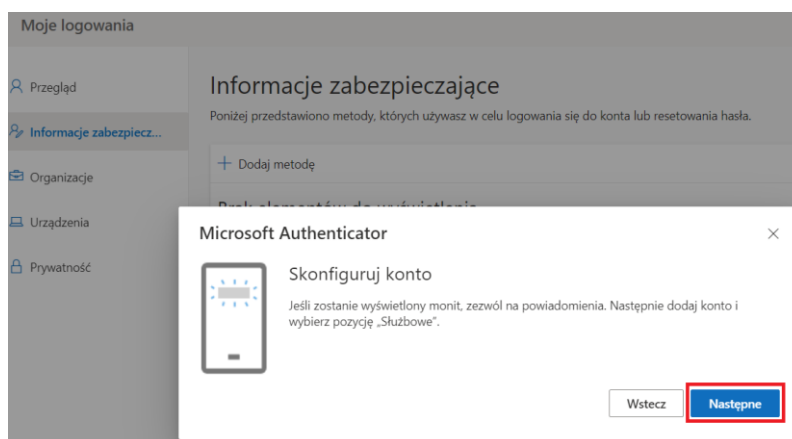
Następnie otworzy się okno, w którym wybieramy metodę drugiego uwierzytelniania. Należy wybrać pozycję *Aplikacja uwierzytelniania*, a następnie kliknąć przycisk *Dodaj*.



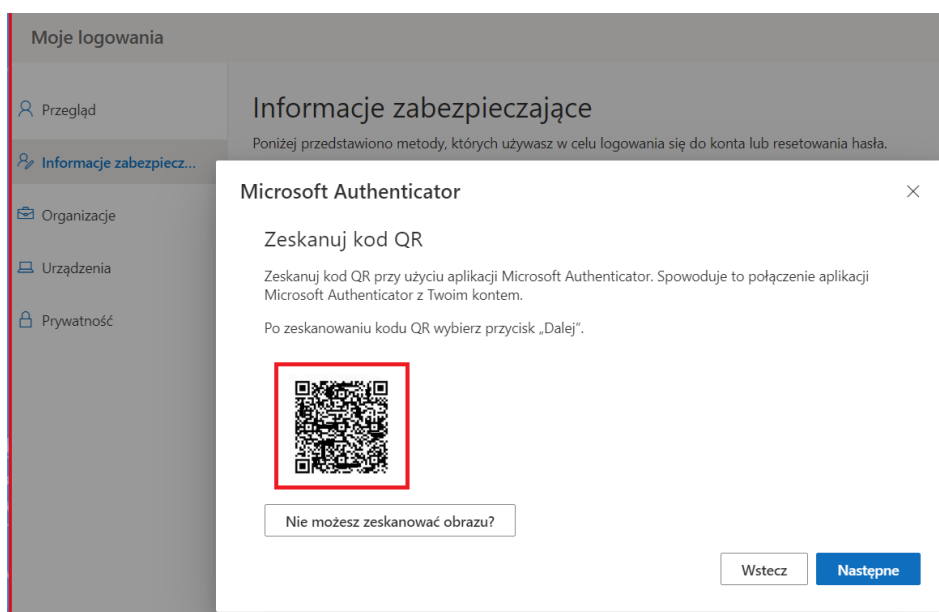
Następnie system poprosi o pobranie aplikacji. Postępując zgodnie z tą instrukcją aplikację na telefonie mamy już zainstalowaną, dlatego wybieramy opcję *Następne*.



W kolejnym kroku również należy wybrać opcję *Następne*.



Wyświetlony zostanie kod QR, który należy zeskanować za pomocą zainstalowanej wcześniej aplikacji Microsoft Authenticator.

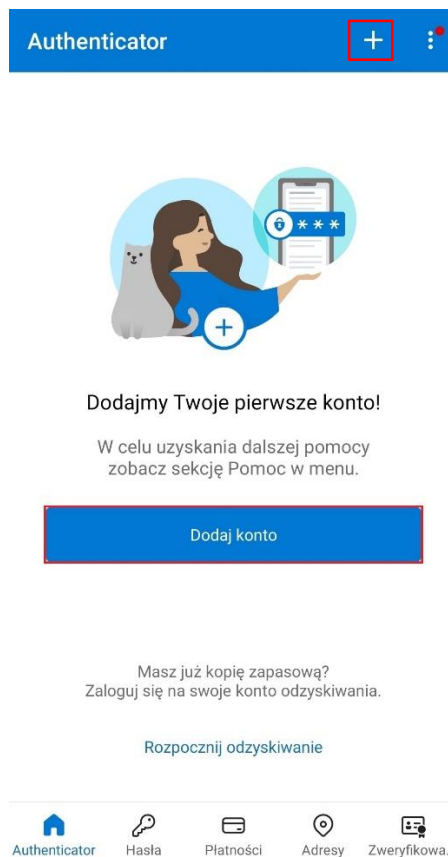


W tym celu należy ponownie uruchomić aplikację Microsoft Authenticator na urządzeniu mobilnym.

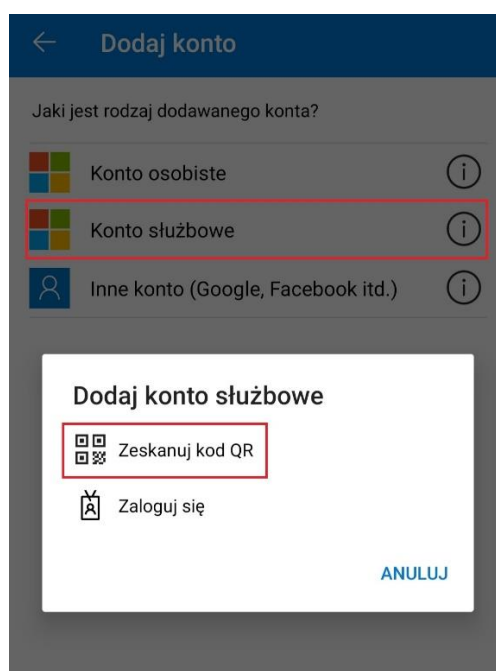
Istnieją dwa możliwe scenariusze wyświetlenia informacji na urządzeniu mobilnym użytkownika.

1. Widok dodawania nowego konta

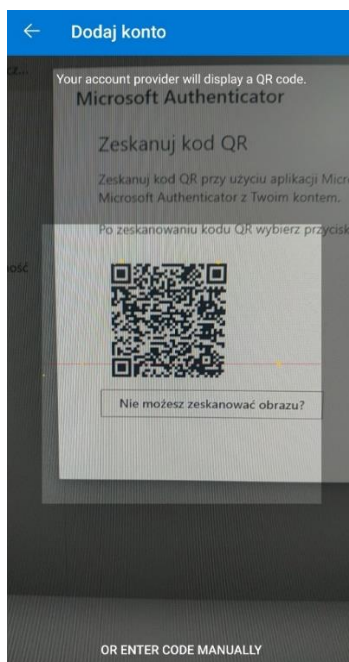
Jeśli wyświetli się poniższy widok należy wybrać *Dodaj konto* lub wybrać ikonę „+”.



Następnie należy wybrać z listy *Konto służbowe*, co spowoduje pojawienie się okna. W oknie należy wybrać opcję *Zeskanuj kod QR*.



Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.



Na urządzeniu pojawić się może komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień aplikacji.* Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie w taki sam sposób w jaki odblokowywany jest ekran telefonu.

Po zeskanowaniu kodu QR należy powrócić do zakładki Informacje zabezpieczające otwartej uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.

Microsoft Authenticator



Zeskanuj kod QR

Zeskanuj kod QR przy użyciu aplikacji Microsoft Authenticator. Spowoduje to połączenie aplikacji Microsoft Authenticator z Twoim kontem.

Po zeskanowaniu kodu QR wybierz przycisk „Dalej”.

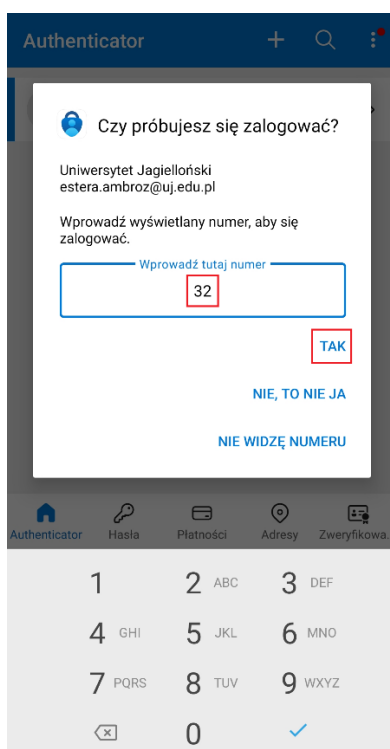
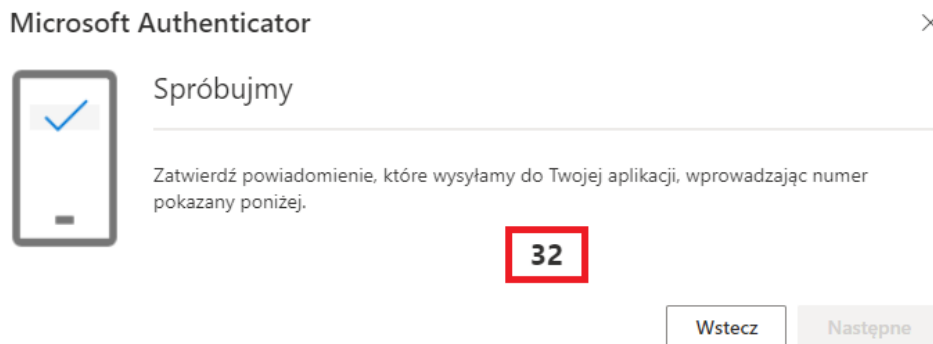


Nie możesz zeskanować obrazu?

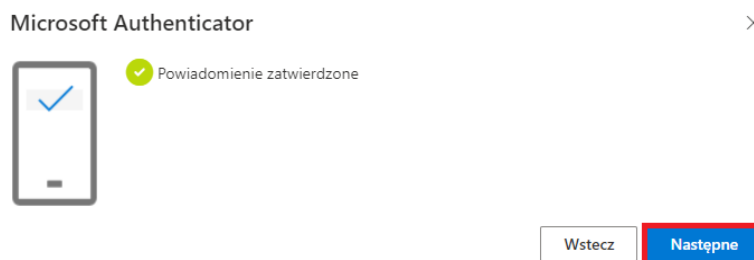
Wstecz

Następne

W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.

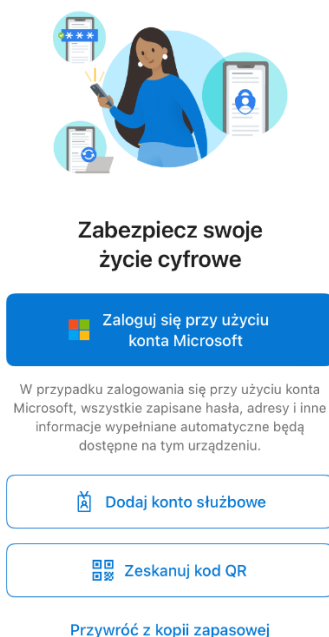


Ostatnim krokiem jest wybranie opcji *Następne* w kolejnym komunikacie wyświetlonym w przeglądarce. Po wykonaniu powyższych czynności metoda powinna zostać poprawnie skonfigurowana.

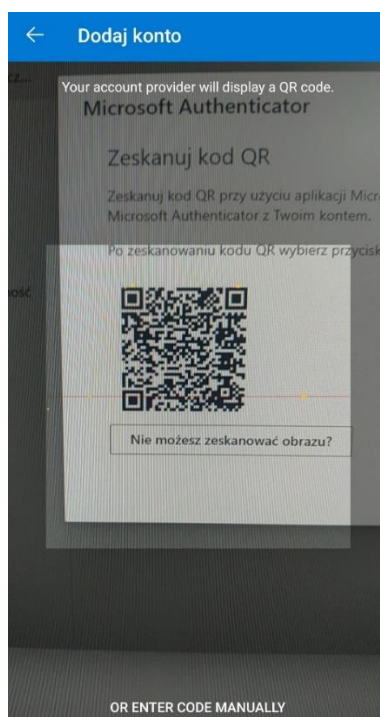


2. Widok wyboru akcji

Jeśli wyświetli się poniższy widok należy wybrać *Zeskanuj kod QR*.



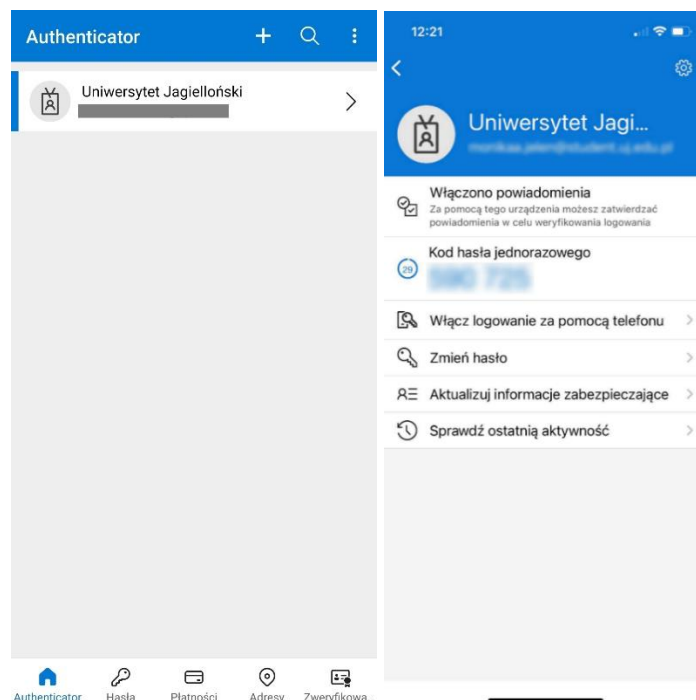
Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.



Po zeskanowaniu pojawia się komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień*

aplikacji. Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie w taki sam sposób w jaki odblokowywany jest ekran telefonu.

Po zeskanowaniu kodu QR w aplikacji mobilnej pojawi się konto uniwersyteckie.



Po zeskanowaniu kodu QR należy powrócić do zakładki Informacje zabezpieczające otwartej uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.

Microsoft Authenticator



Zeskanuj kod QR

Zeskanuj kod QR przy użyciu aplikacji Microsoft Authenticator. Spowoduje to połączenie aplikacji Microsoft Authenticator z Twoim kontem.

Po zeskanowaniu kodu QR wybierz przycisk „Dalej”.

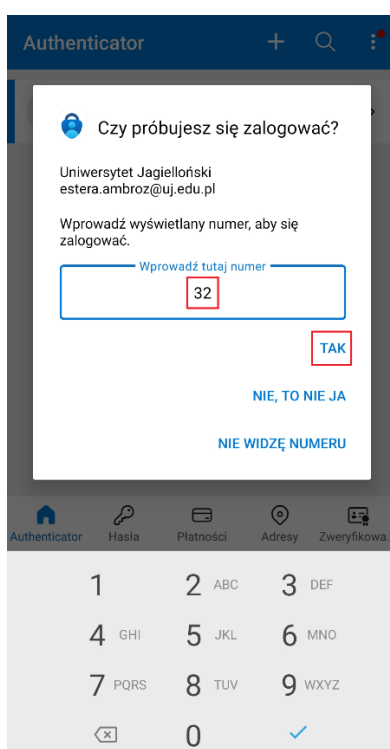
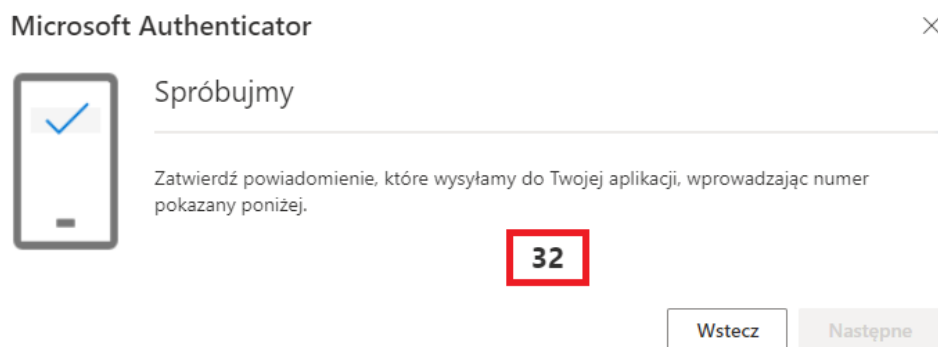


Nie możesz zeskanować obrazu?

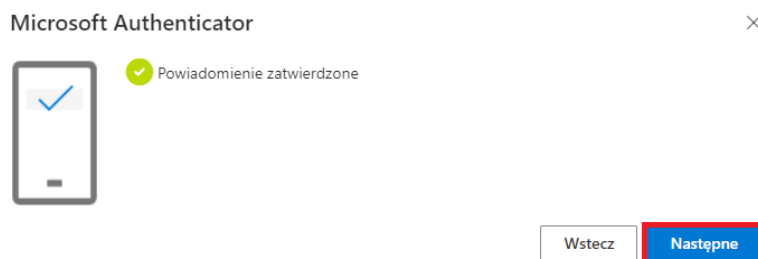
Wstecz

Następne

W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.



Kolejnym krokiem jest wybranie opcji *Następne* w kolejnym komunikacie wyświetlonym w przeglądarce.



Ostatnim krokiem jest wybranie domyślnej metody logowania w zakładce *Informacje zabezpieczające*. Należy wybrać *Uwierzytelnianie oparte na aplikacji – powiadomienie*.

Informacje zabezpieczające

Poniżej przedstawiono metody, których używasz w celu logowania się do konta lub resetowania hasła.

Domyślna metoda logowania: Microsoft Authenticator — powiadomienie [Zmień](#)

Zmień domyślną metodę

Której metody chcesz użyć do zalogowania się?

Uwierzytelnianie oparte na aplikacji — powiadomienie

Wstecz Potwierdź

ETAP 3 - ZGŁOSZENIE GOTOWOŚCI DO WŁĄCZENIA PODWÓJNEGO UWIERZYTELNIENIA

W kolejnym kroku należy zgłosić swoją gotowość do włączenia podwójnego uwierzytelniania wypełniając poniższy formularz:

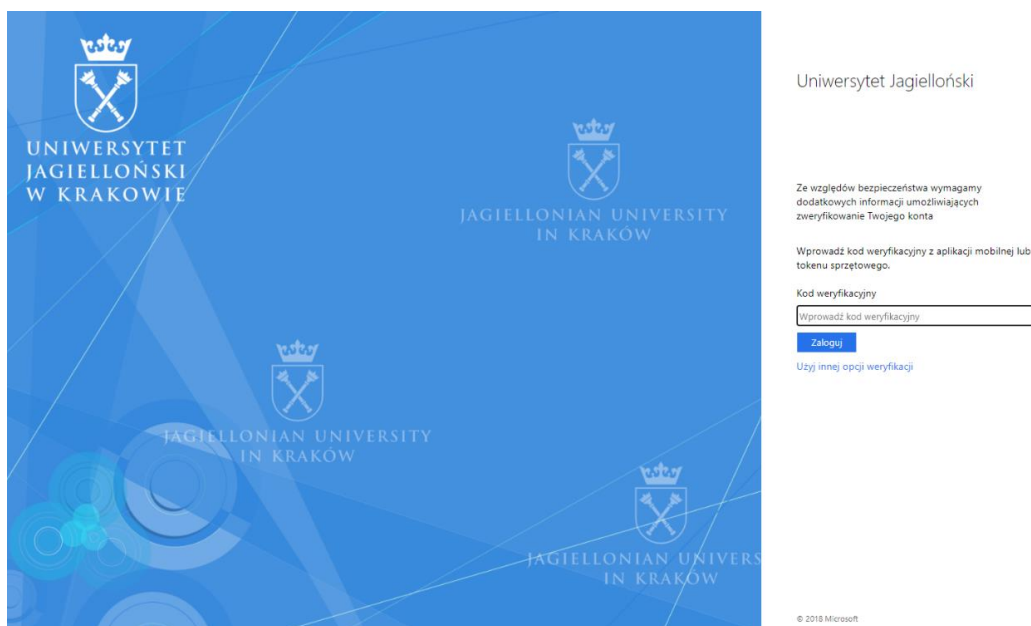
<https://forms.office.com/e/VwsQUUAGsR>

Formularz dostępny jest po zalogowaniu się kontem UJ.

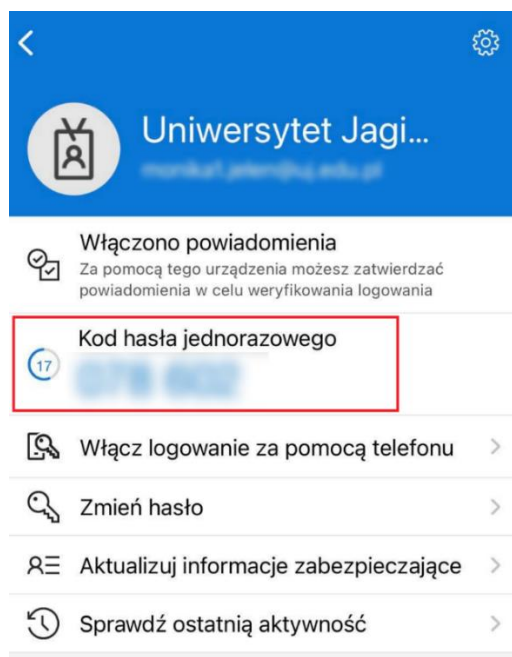
ETAP 4 - LOGOWANIE PO WŁĄCZENIU PODWÓJNEGO UWIERZYTELNIANIA

W ciągu kilku kolejnych godzin aplikacje na komputerze bądź na innych urządzeniach będą zgłaszały prośbę o potwierdzenie logowania drugim faktorem.

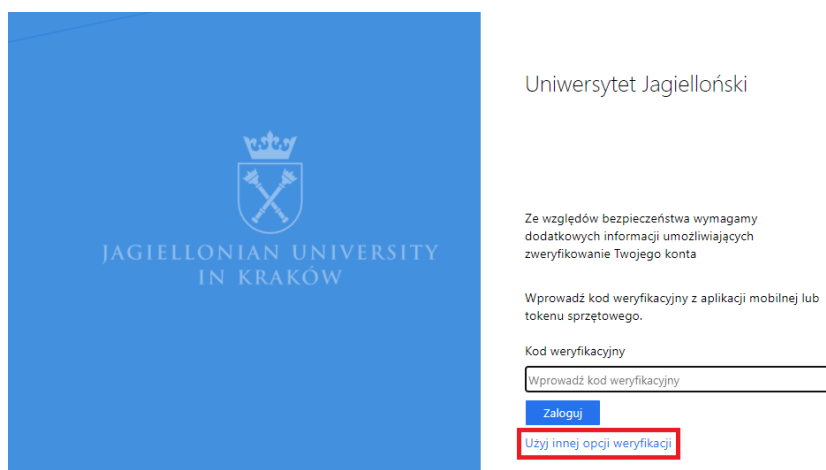
Gdy jesteśmy zalogowani na urządzeniach to zostaniemy wylogowani i poproszeni o ponowne zalogowanie, a kolejno o potwierdzenie logowania w aplikacji Microsoft Authenticator na urządzeniu mobilnym.



Gdy użytkownik zostanie poproszony o wpisanie kodu weryfikacyjnego powinien uruchomić aplikację na swoim telefonie (urządzeniu mobilnym) i wprowadzić wyświetlany kod.



Możliwa jest również zmiana opcji weryfikacji poprzez wybranie *Użyj innej opcji weryfikacji*.



Uniwersytet Jagielloński

Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Wprowadź kod weryfikacyjny z aplikacji mobilnej lub tokenu sprzętowego.

Kod weryfikacyjny

Zaloguj

Użyj innej opcji weryfikacji

Kolejno należy wybrać *Wyślij powiadomienie do mojej aplikacji mobilnej*.



Uniwersytet Jagielloński

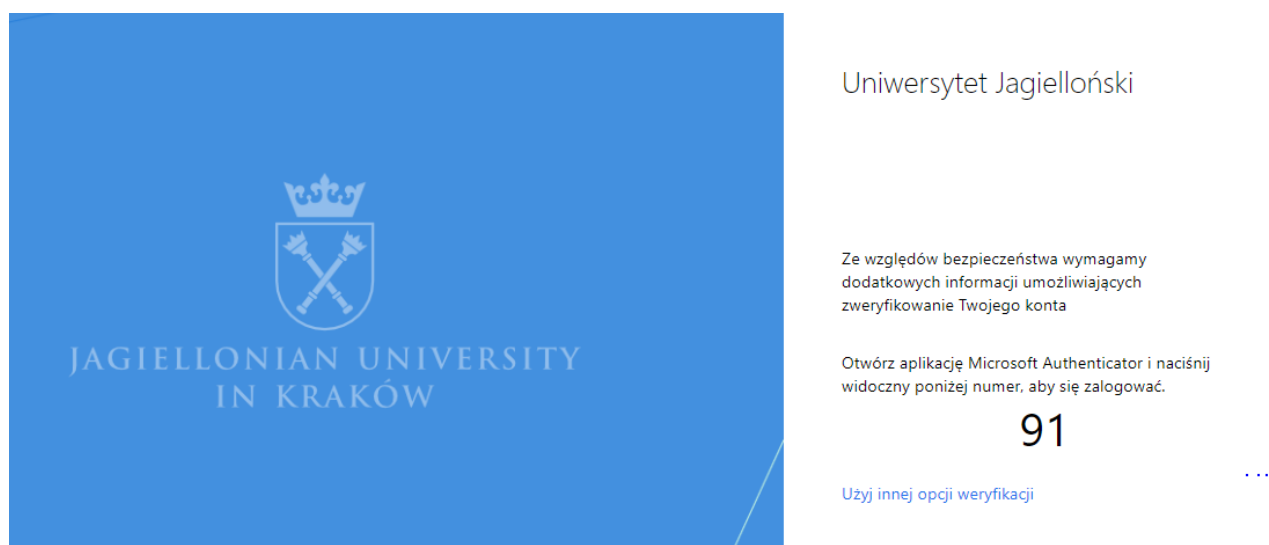
Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Jak mamy zweryfikować Twoje konto?

[Użyj kodu weryfikacyjnego z aplikacji mobilnej lub tokenu sprzętowego](#)

Wyślij powiadomienie do mojej aplikacji mobilnej

Wtedy na ekranie komputera wyświetli się liczba:



Uniwersytet Jagielloński

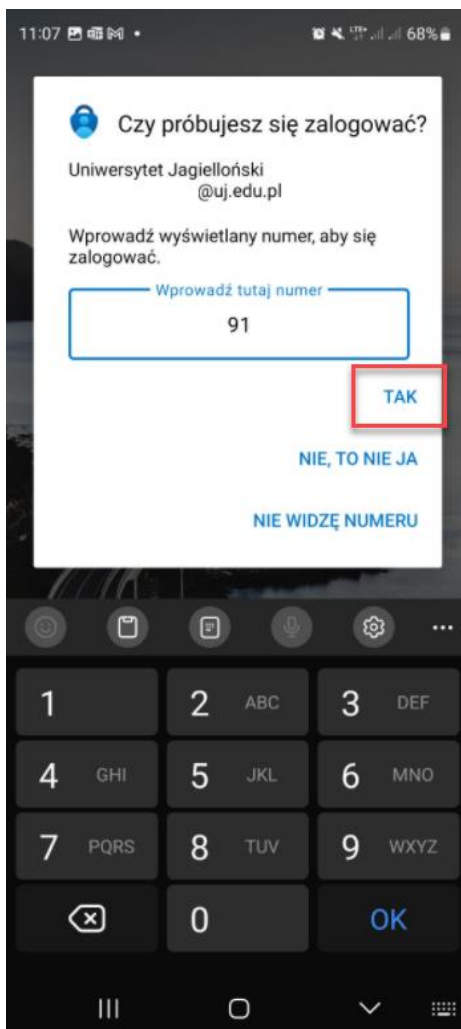
Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Otwórz aplikację Microsoft Authenticator i naciśnij widoczny poniżej numer, aby się zalogować.

91

[Użyj innej opcji weryfikacji](#)

Na naszym urządzeniu mobilnym wyświetli się komunikat, który poprosi o zatwierdzenie logowania poprzez podanie liczby wyświetlonej na ekranie komputera i kliknięcie opcji TAK.




Po wpisaniu liczby należy potwierdzić logowanie wzorem lub kodem blokady ekranu urządzenia mobilnego.

DODATKOWE CZYNNOŚCI WYMAGANE DLA NIEKTÓRYCH URZĄDZEŃ ORAZ APLIKACJI

Dla niektórych urządzeń oraz aplikacji będzie wymagane dodatkowe działanie, aby podwójne uwierzytelnianie zostało w pełni skonfigurowane oraz synchronizacja danych na urządzeniu nie została wstrzymana.

Klient synchronizacji OneDrive

Aplikacja OneDrive instalowana na komputerze do synchronizacji plików z dyskiem chmurowym wymaga po skonfigurowaniu podwójnego uwierzytelnienia ponownego zalogowania się do usługi.

W tym celu należy kliknąć ikonę klienta OneDrive na pasku zadań komputera  a następnie klikając w monit z prośbą o ponowne zalogowanie, zalogować się kontem UJ.

W aplikacji Microsoft Authenticator na urządzeniu mobilnym pojawi się prośba o zatwierdzenie logowania. Po tym zatwierdzeniu aplikacja OneDrive ponownie rozpocznie synchronizację plików z komputerem.